Informação

"Conjunto de dados utilizados para a transferência de uma mensagem entre pessoas e / ou máquinas em processos de troca de mensagens (comunicativos) ou transacionais (transferência de arquivos)."

A política da segurança

A política de segurança de informação é um mecanismo preventivo de proteção dos dados e processos de uma organização e que define também um padrão de segurança a ser seguido pelo pessoal técnico, gerência e pelos demais usuários (internos e externos) do sistema de informação.

Pode ser usada ainda para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais. Uma de suas preocupações é estabelecer os métodos de proteção, controle e monitoramento dos recursos de informação. É importante que a política de segurança defina as responsabilidades das funções relacionadas à segurança e discrimine as principais ameaças, riscos e impactos envolvidos.

A política de segurança deve integrar-se às metas de negócio da organização e ao plano das políticas de informatização, influenciando todos os projetos de informatização da empresa tais como o desenvolvimento de novos sistemas, planos de contingências, planejamento de capacidade, dentre outros. É importante lembrar que a política não envolve apenas a área de tecnologia da informação (TI), mas a organização como um todo.

Como toda política institucional, deve ser aprovada pela alta gerência e divulgada a todos os funcionários e usuários de serviços de informática. A partir de então, todos os controles devem ser baseados nessa política de segurança.

Ameaças

As principais ameaças que devem ser tratadas pela da Política de Segurança da Informação são as seguintes:

- Ameaças à integridade: Ameaças ambientais (fogo, água, terremoto, etc), erros humanos, fraudes, falhas de processamento;

- Ameaças de indisponibilidade: Falhas em sistemas ou nos diversos ambientes computacionais;

- Ameaças de divulgação da informação: Divulgação de informações premeditada ou acidental;
- Ameaças por alterações não autorizadas: Alteração premeditada ou acidental do conteúdo das informações do sistema.

São três os aspectos básicos que um sistema de segurança da informação deve atender para evitar a concretização dessas ameaças:

1. **Prevenção**

- **Proteção de hardware**: normalmente chamado de segurança física, impede acessos físicos não autorizados à infra-estrutura da rede, prevenindo roubos de dados, desligamento de equipamentos e demais danos possíveis quando se está fisicamente no local;

- **Proteção de arquivos e dados**: providenciado por autenticação, controle de acesso e antivírus. No processo de autenticação, é verificada a identidade do usuário. No processo de controle de acesso, só são disponibilizadas as transações realmente pertinentes ao usuário. O antivírus garante a proteção do sistema contra programas maliciosos;

- **Proteção de perímetro**: ferramentas de firewall cuidam desse aspecto, mantendo a rede protegida contra invasões de usuários não autorizados.

2. Detecção

- **Alertas**: sistemas de detecção de intrusos (IDS - Intrusion Detection System) alertam os administradores e responsáveis pela segurança da rede sobre qualquer sinal de invasão ou mudança suspeita no comportamento da rede que possa significar um padrão de ataque. Os avisos podem ser via e-mail, via mensagem no terminal do administrador, etc.;

- **Auditoria**: periodicamente deve-se analisar os componentes críticos do sistema a procura de mudanças suspeitas. Esse processo pode ser realizado por ferramentas que procuram, por exemplo, modificações no tamanho dos arquivos de senhas, usuários inativos, etc.

3. **Recuperação**

- **Cópia de segurança dos dados (Backup)**: manter sempre atualizados e testados os arquivos de segurança dos dados em mídia confiável e separado dos servidores;

- **Aplicações de Backup**: ferramentas que proporcionam a recuperação rápida e confiável dos dados mais atualizados em caso de perda dos dados originais do sistema;

- **Backup do Hardware**: a existência de backup de hardware (servidor reserva, no-break reserva, linhas de dados reserva, etc.) podem ser justificados levando-se em conta o custo de uma parada do sistema e determinando-se a importância da informática para a organização.

Gerenciamento de Recursos de Informação

A segurança de uma rede de computadores é parte integrante do Gerenciamento de Recursos de Informação de uma empresa e deve preocupar-se com a aplicação das proteções (técnicas e administrativas) para minimizar as vulnerabilidades e anular falhas potenciais como:

- Vulnerabilidades: pontos suscetíveis a ataques, causados por uma brecha do software ou hardware, má configuração e administração ou ambos. Podemos citar como exemplo a análise do ambiente de uma sala de servidores de conectividade e Internet com a seguinte descrição: A Sala dos Servidores não possui controle de acesso físico;

- Ameaças: problemas que podem atacar as vulnerabilidades. Normalmente são agrupadas em três categorias: pessoais (omissão ou intenção criminal), de componentes (falha de um equipamento) e de eventos (fogo, inundação). Seguindo o exemplo da Sala dos Servidores, podemos identificar a ameaça da seguinte forma: Fraudes, Sabotagens, Roubo de Informações, Paralisação dos Serviços.

Objetivos do Gerenciamento

A segurança de redes de computadores, dentro do conceito de Gerenciamento de Recursos, visa atender aos seguintes objetivos gerais:

- **Confidencialidade ou sigilo**: proteger contra a revelação acidental ou deliberada de informações críticas. É a garantia de que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede;

- **Integridade**: proteger contra corrupção deliberada ou acidental de informações garantindo que o conteúdo de uma mensagem ou resultado de uma consulta não será alterado durante seu tráfego;

- **Disponibilidade**: proteger contra ações que causem a indisponibilidade de informações críticas aos usuários quando necessitarem;

- **Autenticação**: garantia de identificação das pessoas ou organizações envolvidas na comunicação;

- **Não-Repúdio (Não recusa):** garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá, posteriormente negar sua autoria.